USAO File Number: 2018R00729 AUSA: Hank Moon Telephone: (313) 226-9100

AO 106 (Rev. 04/10) Application for a Search Warrant Special Agent: Jessica Knickerbocker Telephone: (313) 965-2323

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 19-mc-50186-5
6425 Tireman Street, Detroit, MI 48204, and 16332 Horseshoe Drive, Northville, MI 48168, more fully described in Attachments A-1 and A-2.	)	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENTs A-1 and A-2.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. § 7206	Fraud and false statements
18 U.S.C. § 542	Entry of goods by means of false statements

The application is based on these facts:

See attached AFFIDAVIT.

☐ Continued on the attached sheet.

☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jessica Knickerbocker
Applicant's signature

Jessica Knickerbocker, Special Agent, IRS
Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: October 12, 2021

Judge's signature

City and state: Detroit, Michigan

Anthony P. Patti U. S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jessica Knickerbocker, a Special Agent with the Internal Revenue Service and a Task Force Officer with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

EXECUTIVE SUMMARY

Ali Kassem Kain operates Specialized Overseas Shipping (SOS), a freight forwarding business located in Detroit, Michigan. Evidence obtained by CBP during attempted border crossings and pursuant to a federal search warrant of Kain's, SOS's, and other participants' email accounts shows that Kain and SOS are importing vehicles from Canada and are providing fraudulent paperwork to U.S. Customs and Border Protection at the border, in violation of 18 U.S.C. § 542 (entry of goods by means of false statements).

A related investigation into Kain and his businesses, primarily SOS, shows that there are significant inconsistencies in his personal and business tax filings as compared with his personal and business financial information (bank records, credit card transactions, etc.). An analysis of Kain's business and personal tax returns and business and personal bank account activity, obtained via legal process, shows significant discrepancies between his financial transactions and reported tax information: there is probable cause to believe that Kain has significant unreported income and overstated expenses; that Kain has unreported foreign bank accounts

(including an account(s) in Lebanon); and that Kain is using his business bank accounts to conduct non-SOS business and possibly launder illegal proceeds, all in violation of 26 U.S.C. § 7206 (fraud and false statements). These conclusions are supported by the fact that Kain, based on my training and experience, appears to be layering—blending money, including illicit money, from several sources and/or constantly moving money—in an attempt to disguise his transactions and reduce his tax liabilities.

Kain and his businesses operate out of SUBJECT PREMISES 1, and Kain lives at SUBJECT PREMISES 2, where evidence shows he conducts both personal and business activities. Further, his wife Mariam Beydoun, is also an SOS employee and appears to work from SUBJECT PREMISES 2. Therefore, there is probable cause to search both SUBJECT PREMISES 1 and 2 for evidence of these crimes, as further discussed below and in Attachments A-1, A-2, and B.

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search the following locations:

   a. **6425 Tireman Street, Detroit, MI 48204**, the business location of Ali Kain's businesses ("SUBJECT PREMISES 1"); and

   b. **16332 Horseshoe Drive, Northville, MI 48168**, the residence of Ali Kain and Mariam Beydoun ("SUBJECT PREMISES 2"; combined,

the "SUBJECT PREMISES"), further described in Attachments A-1 and A-2, for the things described in Attachment B.

2. I am a Special Agent with the Internal Revenue Service, Criminal Investigation, and have been so employed since August of 2005. As a Special Agent, I have completed training at the U.S. Federal Law Enforcement Training Center in Glynco, Georgia, which covered all aspects of financial investigation, including search and seizure, violations of the Internal Revenue Laws, and Internal Revenue Service policies and procedures. My responsibilities include the investigation of possible criminal violations of the Internal Revenue Laws (26 U.S.C.), the Bank Secrecy Act (31 U.S.C.), the Money Laundering Control Act (18 U.S.C.), and related offenses. During my employment as a Special Agent with the IRS, I have directed or assisted in investigations concerning money laundering, income tax, and Bank Secrecy Act violations. These investigations focused on individuals deriving income from a mix of legal and illegal sources. I have participated in the execution of search warrants involving the seizure of records relating to the concealment of assets and proceeds from fraud. I have received extensive training in accounting and financial investigation techniques and have participated in numerous training classes and seminars on money laundering, the Bank Secrecy Act, and asset forfeiture.

3. The facts set forth below establish probable cause to believe Ali Kassem Kain ("Kain") filed false personal and business tax returns for the years 2015, 2016, 2017, and 2018. Further, the facts set forth below also establish probable cause to believe that since January of 2015, Kain and employees of Specialized Overseas Shipping, his company, have been submitting fraudulent dock receipts to U.S. Customs and Border Protection. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Ali Kain violated Title 26, United States Code, Section 7206 (fraud and false statements) and Title 18, United States Code, Section 542 (entry of goods by means of false statements). There is also probable cause to search the SUBJECT PREMISES, described in Attachments A-1 and A-2, for evidence of these crimes**,** as described in Attachment B. Due to the nature of the alleged offenses and the items described in Attachment B, I request authority to search the entire SUBJECT PREMISES, including any garages, sheds, storage rooms, shipping containers (for vehicles), and/or any outbuildings, as well as all vehicles on the SUBJECT PREMISES that law enforcement reasonably believes belong to Ali Kain or one of Kain's businesses.

4. The information in this affidavit comes from numerous sources including, but not limited to, my own personal observations and participation in this investigation and my review and analysis of oral and written reports and

documents. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

Background

5. There are two related investigations involving Ali Kain. First, the IRS is conducting a criminal investigation with the Federal Bureau of Investigation in Detroit and Albany, New York, into Kain and his business, Specialized Overseas Shipping, submitting fraudulent documents to U.S. Customs and Border Protection. Second, The IRS is conducting a criminal investigation of Ali Kain's personal and business tax returns for the years 2015, 2016, 2017, and 2018. The IRS is working jointly with the Canada Revenue Agency (CRA) on this investigation, which involves possible inflated business expenses and unreported income. Both investigations focus on Kain and his businesses, primarily Specialized Overseas Shipping.

6. Kain operates a freight forwarding business headquartered in Detroit, Michigan—Specialized Overseas Shipping ("SOS"). Kain is the Resident Agent of SOS, and through SOS, facilitates the shipment of vehicles and other goods throughout the United States and internationally. Kain also owns two additional

businesses—SOS Transportation, Inc. and SOS Realty, LLC, both co-located with SOS at the 6425 Tireman address (SUBJECT PREMISES 1).

7. In 2011, Kain reached a civil settlement with the government in the Southern District of New York (USAO SDNY). According to the Stipulation and Order of Settlement filed with the Court on December 15, 2011, Kain acknowledged that he had "been made aware of the allegations of a scheme to launder the proceeds of violations of IEEPA and proceeds of narcotics transactions through the United States used car market as set forth in the Complaint, including through the purchase of used cars in the United States, their subsequent shipment to West Africa, their sale, the commingling of the proceeds of those sales with narcotics proceeds, and transportation of those funds into Lebanon; and allegations that Hezbollah members and supporters are involved at various points in the money laundering scheme."

8. As a result of the civil settlement, Kain was ordered to forfeit "all funds on deposit in the Comerica Bank Accounts, held in the name of Global Shipping Services," Kain's business at the time of the 2011 settlement. Additionally, Kain was ordered that he "shall not enter into any transactions with any party who he has reason to believe is affiliated with Hezbollah."

9. SOS operates primarily in the United States, Canada, and West Africa. Global Shipping Services also operated in the United States and West Africa.

10. It has been the assessment of the U.S. law enforcement and intelligence community for the past twenty or more years that foreign terrorist organizations use international shipping routes between the United States and West Africa as a source of funding and money laundering for their global operations. One of the methods most used by these organizations is the purchase, transportation, and sale of used and salvaged vehicles, which are purchased from private sellers, scrap yards, and at auction within the United States, shipped to West Africa, and resold at an inflated value. Proceeds from these sales are then commingled with money obtained from unlawful activities in which many of these organizations engage (often drug trafficking). In some cases, the vehicles being shipped have been stolen from their rightful owners. In order to transport these vehicles from the United States to West Africa, sellers use freight forwarding and export companies—like Global Shipping Services and SOS.

The investigation into false documents

11. As will be detailed later in this affidavit, witness statements, subpoenaed documents, email search warrant results, and the inspection and

comparison of seized documents with other evidence, indicate that SOS often submitted dock receipts that were altered (suspected fraudulent) to U.S. Customs and Border Protection (CBP) when importing and exporting vehicles through third-party carriers. As described by witnesses and confirmed by a review of the records obtained in this case, when importing and exporting vehicles, SOS repeatedly submitted fraudulent dock receipts to CBP to save on bond fees, obscure the shippers of stolen vehicles,[1] and promote other fraudulent activity.

12. In this context, SOS operates as a freight forwarder/vehicle broker: SOS is responsible for filling out the dock receipts; booking the shipment with the transportation company (the company that physically transports the vehicles to the port, like Sweetie Boy Trucking, discussed below); and booking the shipment with the carrier (the company that transports the vehicle from the port overseas and completes the dock receipts). Records provided by CBP and records obtained via email search warrant (discussed in detail below), accompanying hundreds of

[1] To date, the FBI and CBP have identified and seized at least twenty-four vehicles stolen in Canada that SOS imported or attempted to import into the U.S. between May 2017 and April 2019. And there were likely more, because within twenty-four hours of a vehicle being stolen in Canada, the people responsible for the thefts were able to change the Vehicle Identification Number (VIN) on the stolen vehicle, produce fraudulent paperwork, send the paperwork to a freight forwarding company (in the automobile context, sometimes called a vehicle broker), and transport the vehicle to the U.S. port of entry. This speed likely enabled the organization to move the vehicle through inspection at the U.S. port of entry before the theft was officially reported and registered in law enforcement databases.

vehicles from Canada into the U.S. in total—and all twenty-four stolen vehicles discussed in footnote 1—list SOS as the freight forwarding company.

13. In March of 2017, CBP inspected SOS's vehicle holding lot in Canada. Inspecting officers spoke with Malek Tahan, an SOS employee and Canadian resident who managed SOS's Canadian lot. Tahan admitted that he was giving Sweetie Boy Transportation two sets of documentation (also called "dock receipts") for each vehicle. One set was given to CBP when the vehicles entered the United States from Canada, and the other set accompanied the vehicles on a ship from the United States to its final destination, usually in West Africa.[2]

14. The two sets of documents were different, even though they concerned the same vehicles: the set for CBP limited the number of recipients in the United States in order to save on import or "bonding" fees (this false/fraudulent information violates 18 U.S.C. § 542). The set of dock receipts accompanying the vehicle on the ship to West Africa contained accurate information so that each vehicle could be matched to the correct recipient upon arrival. Agents later

[2] According to interviews with two trucking companies doing business with SOS, including Sweetie Boy, SOS changed this procedure after the March 2017 inspection. After that inspection, drivers received the dock receipts for the U.S. to Africa leg via e-mail or via fax after entering the U.S. Thus, inspectors at the border between the U.S. and Canada would not be able to see the inconsistencies in the paperwork (dock receipts). Interviews with a second trucking company confirmed this change. Drivers from both trucking companies complained to their leadership about SOS requiring them to carry two sets of documents.

interviewed a former SOS co-worker of Tahan (herein after, "Interviewee 1"). Agents asked Interviewee 1 why SOS would ship cars with two sets of documentation. Interviewee 1 said that the two sets of documents with different information were used to save money: CBP charges freight forwarding companies a "bond" for each individual shipping company for whom they are forwarding a vehicle. This bond can be anywhere between $35 and $80. Trucks often carry vehicles shipped by several different shippers; but to avoid paying several bonds on each load, freight forwarding companies like SOS will fraudulently claim that all of the vehicles belong to one shipper and thus pay only one bond.

15. Interviewee 1 also told agents that the two sets of paperwork/dock receipts were sent to Tahan from the SOS office in Detroit. Interviewee 1 stated that "Ed" demanded this procedure. "Ed" is known by your affiant to be Ahmad "Ed" Kain, Ali Kain's brother and an SOS employee.

16. After receiving this information, agents obtained a federal search warrant for email accounts associated with SOS employees, Ali Kain, "Ed" Kain, and several trucking company email accounts, among others. An analysis of these email accounts confirmed that SOS was providing two sets of documents/dock receipts for vehicles coming into the United States from Canada and then shipped overseas from the United States—often to West Africa.

17. From the analysis of the email search warrant data, your affiant determined that emails with a subject line including the term "mix load" indicated that SOS provided two sets of dock receipts and therefore likely submitted false information to CBP. A review of the email accounts shows that there were more than 950 emails with "mix load" in the email header line between January of 2015 and January of 2019. Here is a typical example:

a. On March 6, 2017, Ed Kain emailed ten dock receipts attached as PDF files to Sweetie Boy Transportation and SOS employees Malek Tahan, Christina Kazarian, and Ali Dourra: the subject line was "MIX LOAD # 109/MONTREAL TO BAYONNE." Approximately 30 minutes later, Hala Siblani, another SOS employee, sent an email to Tahan, Ed Kain, and Ali Dourra—all SOS employees—with the subject line, "LOAD# 109 FOR OUR RECORD." This email contained dock receipts as PDF attachments that were different versions of those in the first email—but for the same vehicles. For example, the dock receipt with filename HBL17-2224.pdf listed the exporter as Auto Adan in the intra-SOS email, while the dock receipt for the same vehicle provided to Sweetie Boy listed Ghaddar General Trading. Likewise, the dock receipt with filename HBL17-2227.pdf listed the exporter as El H Auto in the intra-SOS email, while the dock receipt for the same vehicle provided to Sweetie Boy again listed Ghaddar General Trading.

18. Agents reviewed the electronic copies of paperwork for approximately 50 of these vehicles—imported by SOS from Canada into the U.S., and then exported (or attempted exported) from the U.S. overseas—found in these email accounts and learned that SOS provided two sets of dock receipts for the same vehicles. This was true for both stolen and not stolen vehicles.

19. A review of these email accounts also show that SOS changed the name of the "exporter" from Canada on many of the dock receipts for vehicles later identifies as stolen—which protected the name of the people stealing the cars if the theft was identified at the border. For example, the dock receipt with filename HBL17-2227.pdf, identified above, was for a 2006 Mercedes, later determined to be stolen in Canada. The exporter identified in SOS's records was El H Auto, while the dock receipt for the same vehicle provided to Sweetie Boy listed Ghaddar General Trading as the exporter. In addition to saving SOS money (by listed Ghaddar General Trading as the exporter for many vehicles on the paperwork provided to CBP at the border), the change of exporter concealed the true exporter for the stolen Mercedes and shielded the exporter from discovery by law enforcement.

20. In another example, a 2017 Acura MDX was determined to be stolen in Canada and subsequently seized by CBP at the border. The exporter on the dock receipt that SOS provided to Sweetie Boy (and which Sweetie Boy later provided to CBP) was A & K Import; however, the vehicle registration that accompanied the stolen Acura indicated the registrant was 9309-4462 Quebec Inc. In SOS records (including Ali Kain's email account), 9309-4462 Quebec Inc. was also listed as the actual exporter, not A & K Import. On April 3, 2018, a U.S. Customs summons was served on SOS for the stolen Acura's associated paperwork. A review of

SOS's email accounts show that SOS subsequently requested this paperwork from Sweetie Boy Transportation. It is believed this was done to ensure that SOS provided U.S. Customs the same, fraudulent version that Sweetie Boy provided to CBP rather than the accurate version maintained by SOS (that would show that SOS was providing two copies of dock receipts).

21. On July 25, 2019, agents interviewed the owner of A & K Import, who confirmed that he did buy cars in Montreal, that he used Ali Kain's shipping company, and that Kain's SOS lot was managed by a man with the first name Malek. The owner stated, however, that he never bought an Acura MDX in Canada and shipped it to the U.S.—in contradiction to the dock receipt provided by Sweetie Boy to CBP.

The tax return investigation

22. Kain files his personal tax returns jointly with his wife, Mariam Beydoun, who is also an employee of SOS. Kain owns three companies all located at SUBJECT PREMISES 1: Specialized Overseas Shipping (SOS), doing business as SOS Shipping; SOS Transportation, Inc., and SOS Realty, LLC. A review and analysis of Kain/Beydoun's personal and business tax filings shows significant inconsistencies with their personal and business financial transactions. Specifically, an analysis of Kain/Beydoun's personal tax returns for the years 2015

to 2018 show that they received more funds than what was reported on their personal tax returns filed with the IRS. Further, an analysis of Kain's business tax returns and business bank account activity shows significant discrepancies, primarily unreported income and overstated expenses. Based on my training and experience, Kain/Beydoun's personal and Kain's business tax returns are not accurate for the yeas 2015 to 2018, as further explained below.

A. Kain's business financial information and discrepancies

23. Kain operates three businesses according to IRS records, all out of SUBJECT PREMISES 1: Specialized Overseas Shipping (SOS), doing business as SOS Shipping; SOS Transportation, Inc.; and SOS Realty, LLC. SOS Realty did not make any tax filings with the IRS from 2016 (the first year after it was formed) through 2019. Specialized Overseas Shipping reported the following gross receipts (gross sales) and ordinary income/loss:

	2015	2016	2017	2018
Gross receipts:	$7,961,515	$3,107,140	$3,906,245	$6,945,817
Ordinary income:	$47,197	$6,176	$31,414	-$53,224

24. Based on my review of these tax records, the net profits (ordinary income/gross receipts) for SOS were unusually low: .59% in 2015; .20% in 2016; .80% in 2017; and -.77% in 2018 (comparatively, The IRS website states that

average net profit for businesses in the "air, rail, and water transportation" industries is about 8.47%).

25. Further, Kain regularly "loans" money from SOS to "shareholders"—himself—without increasing his wages. Kain reported a personal income from SOS of $137,221 in 2016, $135,368 in 2017, and $119,600 in 2018. Yet, tax filings show that Kain received an additional $77,981 in 2016, $63,081 in 2017, and $87,047 in 2018 in "loans"—which were not reported as personal income. Based on my training and experience, shareholders often take "loans" from their business to avoid paying taxes. In 2017 an underwriter (lender) asked Kain about SOS's loans to shareholders and why these loans were taken out. Kain responded:

> this money is a combination of personal withdraws over the past 4 years. Most of it was to pay for 2 life insurance policies (over $40k per year), house upgrades, among other needs. I had the choice to consider it income and has it taxed or take it as a loan hoping to get it offset during a highly profitable year. Most likely, we will start partially break it as annual income over the next few years. We have not decided yet. I do not feel bad about, I built this company from ZERO and the early years, I put lots of injections into it. If any, it shows that the company was and continues to be profitable. I own it 100%.

26. Bank records also show that SOS received hundreds of thousands of dollars in "loans" from others: $90,500 in 2015, $60,000 in 2016, and $233,000 in 2017. These funds were deposited into SOS's account and referenced "loans" on the memo (subject) line of the deposit. Most of this money came from businesses

belonging to Kain's brothers-in-law (who also deposited an additional $120,000 into SOS's account with nothing written on the subject line of the deposit). Based on my review of the documents in this case, there is no evidence that any of these individuals shipped vehicles through SOS, and financial records do not indicate that SOS has made payments on any of these loans. Based on my training and experience, I know that money can be described as "loans" with the recipient never actually paying back the loans—becoming, therefore, improper unreported income.

27. In addition to loans, tax and bank records show that Kain used his business credit card to pay personal expenses, including personal property taxes and personal IRS tax payments (without reporting these figures as income). Likewise, Kain regularly pays his life insurance premiums from his business bank accounts (without reporting these figures as income), even though—for tax purposes—he considers his life insurance policy as a personal asset. For example, Kain claimed his life insurance policy as a personal savings account when applying for a business loan in 2016. Kain also listed his life insurance's cash value as an asset on a personal financial statement in 2015.

28. Kain also provided false information to lenders to obtain large sums of money allegedly for business reasons that he ultimately uses for personal reasons. For example, in 2017 Kain obtained a $242,000 loan from Funding Circle with a monthly payment of $8,555. In an email to Funding Circle dated September

28, 2017, Kain said that he planned to use the funds for working capital. In early 2018, Kain applied for a business loan with Straight Line Source—but the loan was denied. In an email exchange with a Straight Line Source branch manager, Kain said that he didn't have to tell the truth about taking the $250k loan from Funding Circle, which ultimately went to his brother. Kain stated: "but the truth is, I have never taken a loan at high interest in my life. My brother started a small business and needed help and no one would give him a loan because his company is new and had no history. He asked me to assist him and he would pay this short term loan. I did. Whether the loan is for SOS or my brother, who cares, as long as it is under SOS Shipping. Good or bad, the loan is there."

29. SOS Transportation's tax and financial records also show significant discrepancies. SOS Transportation reported a loss on its taxes for every year between 2016 and 2019:

	2016	2017	2018	2019
Gross receipts:	$23,330	$42,555	$21,062	$0
Ordinary income:	-$1,238	-$4,797	-$7,020	-$18,515

30. A review of Kain's business tax records show that Kain "loaned" SOS Transportation $33,000 in 2016, but bank records show that Kain only "loaned" SOS Transportation $16,000—from SOS's bank account.

31. Bank records show that SOS Transportation had a single bank account and that Kain and his brother, Ahmad Kain, were the signatories on the account. The account was opened on June 13, 2016 and closed on approximately September 30, 2019. Based on my training, experience, and my analysis of these accounts, the bank account did not contain any regular business income or expenses. Total deposits were $40,306 in 2016, $42,255 in 2017, $34,562 in 2018, and $16,380 in 2019, and most of these deposits came from SOS bank accounts or F&A Trucking, a company owned by Kain's brother-in-law. Most of the deposits from F&A Trucking were labeled "payroll." Most of the withdrawals from the account were to pay an SOS Transportation loan, although there was also a $10,000 business check written in 2016 to Ahmad Kain for "personal loan." There were no payments indicating that Ahmad repaid this loan. Finally, my analysis of SOS Transportation's accounts show that deposits into its bank account exceeded reported gross receipts during the 2016 to 2019 period by approximately $30,000—with no explanation for the discrepancy.

32. Finally, my review of the records and communications in this case suggests that Kain has foreign bank accounts and foreign income that he has not reported with the IRS, rendering his tax returns inaccurate. For example, Kain exchanged an email in January 2019 with Mohamad Imad Khalil of Bank Med in Lebanon regarding Kain's Bank med loan balance of $277,730. Kain took out the

loan in 2017 and made the first payment in August 2017. In 2019, Khalil wrote to offer Kain a new, lower monthly payment on his remaining balance of $64,000. Yet Kain's U.S. bank accounts do not show any payments made to Bank Med in Lebanon, and there is no indication in his financial information of where the $213,730 Kain paid to Bank Med came from.

33. Further, in an email dated February 1, 2018, with a branch manager of Straight Line Source regarding an SOS loan application, Kain admitted that "most of our sales are collected by our vendors at overseas destination via their agents. So, only a fraction comes back to after they deduct the cost." SOS does a large amount of business in Africa, and SOS agents in Africa regularly pay SOS expenses. For example, records obtained show that SOS paid Atlantic Container Lines (a shipping company) $1,859,716 from January – October 2017. Of that, more than $600,000 came from SOS agents in Africa. Yet, looking at SOS's tax filings, there is no indication that any income earned overseas and deposited in a foreign bank account is included on SOS's tax returns as gross receipts. That is true despite the fact that SOS bank deposits exceed SOS's reported gross receipts (for tax purposes) by $276,754 in 2015, $109,105 in 2016, and $90,897 in 2017. In 2018, tax return gross receipts exceed bank deposits by approximately $800,000. More information is needed to determine if expenses paid from SOS's agents in Africa are being deduced from SOS's tax returns.

34. Further evidence suggesting that Kain has foreign bank accounts and foreign income that he has not reported with the IRS can be seen by comparing the number of vehicles Kain shipped each year with the gross receipts reported on his tax returns. A review of Kain's shipping records for 90 vehicles that he shipped for one particular client, MEG, between 2019 and 2021 shows that it costs $940 on average to ship a vehicle overseas. Yet, comparing the number of vehicles Kain/SOS shipped each year with the gross receipts for those years reported on SOS's tax returns show that SOS is not reporting enough money to even cover the costs of shipping the vehicles (much less pay salaries, overhead, and other expenses). Based on my training and experience, this indicates that SOS potentially has unreported income—likely in an unreported foreign bank account(s):

	Tax return gross receipts	# vehicles exported	Gross receipts/vehicle
2014	$15,885,143	18,019	$881.58
2015	$7,961,515	13,494	$590
2016	$3,107,140	4,606	$674.59
2017	$3,906,245	6,891	$566.86
2018	$6,945,817	10,714	$648.29
2019	$6,437,221	12,465	$516.42

35. Finally, additional evidence suggests that Kain is using his SOS bank accounts to conduct non-SOS business and possibly launder illegal proceeds. SOS bank records show that an individual with initials K.S. deposited $33,000 into an SOS bank account in 2020. When agents spoke with K.S. she admitted that she never shipped a car or did any business with SOS. Rather, K.S. said that she met a

man on an online dating app in February 2020. The man told K.S. that he was stranded overseas in India and needed money to get home; he convinced K.S. to provide him $50,000, which she did, via MoneyGram, Cashapp, and by depositing $33,000 into SOS's bank account. When asked about that account, K.S. stated that the man provided her with the account number and directed her to deposit money into the account. From my analysis of SOS's accounts, the funds from K.S. appear to be comingled as normal business funds and were used to pay business expenses.

B. Kain's personal financial information and discrepancies

36. Kain's personal tax returns report wages from SOS in the amount of $125,123 in 2015, $137,221 in 2016, $135,368 in 2017, and $119,600 in 2018. Further, according to tax return information, Kain's wife Mariam Beydoun is also employed and paid by SOS. Here SOS income was reported on her jointly filed tax return with Kain. Beydoun's SOS wages were $53,000 in 2015, $48,100 in 2016, $35,000 in 2017, and $36,400 in 2018. Kain and Beydoun's personal tax filings appear inconsistent with the amount of money they received from SOS, including the "loans" described above.

37. For example, Kain and Beydoun's combined personal income in 2015 was reported to be $178,123; but a review of their personal bank account information showed that personal deposits in their bank account in 2015 totaled approximately $302,540. In addition to payroll deposits, deposits into their

personal accounts included $37,479 from AAA insurance proceeds, $25,000 in New York Life Insurance proceeds, and other smaller deposits. The funds from New York Life Insurance were moved from their personal accounts and into SOS's bank account—the check memo on the transfer reflected "loan." The status of the loan to SOS is unknown, but there was no loan from "shareholder"—here, Kain—reflected on the 2015 tax return balance sheet, as there should have been if this were a proper loan.

38. Based on my training, experience, and an analysis of Kain's personal 2015 tax filings, I believe that Kain had approximately $39,000 in unreported income and disbursements in 2015. Further, SOS's 2015 bank accounts show that there was an additional $12,500 issued to Kain personally that was not deposited into his personal bank accounts and was not reported as income on his tax returns.

39. Based on a similar analysis of Kain's financial information for 2016, 2017, and 2018, there also appears to be unreported income and disbursements in those years as well: approximately $41,000 in 2016, approximately $35,000 in 2017, and approximately $117,000 in 2018.

40. After reviewing all of the tax and financial records in this case, and based on my training and experience, I believe that Kain uses layering—blending money, including illicit money, from several sources and/or constantly moving money—in an attempt to disguise his transactions and reduce his tax liabilities. It

is common for individuals who are involved in illegal activity and/or tax fraud to layer transactions to disguise the source of funds.

41. For example, on June 6, 2016, Kain deposited a check from SOS into his personal account in the amount of $11,000; the check said "disbursement" on the memo/subject line. On the same day, he made a $9,454 payment from his personal bank account to his personal Bank of America credit card. A few days later he, took a credit card advance from this same Bank of America credit card in the amount of $16,000 and deposited into his SOS Transportation business bank account. A portion of that money was then used to make a payment on an SOS Transportation loan ($9,087); another portion ($10,000) was paid to his brother, Ahmad Kain—the check said "loan" on the memo/subject line.

42. In another example, Kain took a $15,000 cash advance on September 15, 2016, from SOS's business line of credit. Kain deposited the check into SOS's bank account; a few days later, Kain wrote himself a check for $7,500 and deposited the money into his personal account bank account. He then made a $5,200 payment on his personal credit card and then made some large purchases with his credit card, including buying several plane tickets. This $7,500 was not included as income on his personal tax filings.

43. In a third example, records show that Kain made a payment of $10,000 on December 6, 2017, on a personal credit card (Bank of America). The

payment came from a balance transfer from a different personal credit card (Comerica Bank). On December 14, 2017, Kain took a $15,000 advance from the Bank of America card and deposited the proceeds into his personal bank account at Chemical Bank. On December 19, 2017, KAIN wrote a $8,000 check to his son, Kasem Kain, with the memo line "loan." Kasem Kain then transferred $5,000 of the funds to his Coinbase virtual currency account.

44. From my training and experience, I know that individuals often use their cellular phones to conduct business and personal matters. Evidence obtained from a court-authorized search of Kain's email account shows that Kain regularly uses his cellular telephone to conduct SOS business using email, voice, and messaging platforms, primarily WhatsApp.[3]

45. Regarding email, your affiant has reviewed dozens of SOS-related work emails that Kain sent with "sent from my iPhone" included at the bottom of

[3] WhatsApp is a U.S. company that provides an Internet-basedmultimedia messaging service, WhatsApp Messenger, via a cross-platform smartphone application that permits users to send and receive messages and calls. The smartphone-based WhatsApp Messenger allows users to exchange, inter alia, text messages, audio messages, video messages, and files such as documents and photos with other WhatsApp users. It also permits users to engage in real-time voice and video calls and to set up and participate in group chats. A user may use a cellular provider's data network or another data connection (such as a home wireless router or a public wireless hotspot) to which the user's device is connectedto connect to and send messages via WhatsApp Messenger. WhastApp also permits users of its smartphone application to access their WhatsApp accounts via a desktop or laptop computer.

the message. For example, on January 18, 2018, Kain forwarded an email from his cell phone to an SOS employee instructing an employee to reach out to the carrier to confirm the vehicle was on hold by Customs. The original email that he forwarded was from Malek Tahan. In a second example, on September 30, 2017, Tahan sent Kain an email stating that he collected funds relating to three vehicles that were seized. Kain sent an email from his phone responding to Tahan the next day—October 1, 2017.

46. Further, Kain regularly conducted SOS business on WhatsApp using his cellular phone. For example, records obtained via legal process show that Kain exchanges approximately 105 WhatsApp messages with the owner of Sweetie Boy Transportation between June 2018 and May 2021. Kain also used WhatsApp to conduct business with international shippers. For example, in April 2018 Kain emailed a shipping company specializing in transporting vehicles from the U.S. to West Africa about tracking cargo, among other things. In this email, Kain told the shipping company representative to call him, provided a phone number, and said that he was available on WhatsApp. In a second example, in May 2017, Kain emailed with an agent of a shipping company and stated that he sent a message and the manifest to the agent's WhatsApp account. In a third example, during Kain's email exchange in January 2019 with Mohamad Imad Khalil of Bank Med in Lebanon regarding Kain's Bank med loan balance (see paragraph 32), Kain tried to

have Khalil call him on WhatsApp number to discuss the matter. In a fourth example, a representative from a shipping company sent Kain a WhatsApp message saying that "heard Kain's whatsapp message"; the representative then discussed commission on a project in West Africa. In a fifth example, Kain exchanges a series of emails with a shipping company about shipping vehicles to Nigeria. At one point in the messages, Kain asks the shipping company representative to provide a WhatsApp phone number for Kain to contact them on.

47. From my training and experience, I am familiar with how electronic devices and mobile communication devices can be used to keep, store, and preserve electronic images, location information, contact information, metadata, and other electronic material that may be relevant to a criminal investigation and to establish identify, the location and designs of other conspirators, and the location of other relevant evidence.

THE SUBJECT PREMISES

48. Surveillance conducted between May 2018 and July 2021, in addition to other evidence and public records that I have reviewed, confirms that Kain's main place of business is located at 6425 Tireman, Detroit, Michigan (SUBJECT PREMISES 1). There is an office on SUBJECT PREMISES 1 where surveillance shows (and an interview with Kain confirms) Kain and SOS employees conduct their business. Agents saw several vehicles in various states of disrepair located in

the lot on the west side of the property. Surveillance also showed trucks hauling vehicles being loaded with approximately ten vehicles at a time in the lot and transported off of the property. Agents also saw containers backed into the garage doors of the business and later transported off of the property. It was confirmed those containers were then transported to U.S. ports to be shipped overseas. According to CBP, vehicles shipped overseas often have the relevant paperwork (purchase agreements, dock receipts, titles, etc,) inside. Thus, there is probable cause to believe that records and evidence further described in Attachment B will be located in SUBJECT PREMISES 1.

49. Surveillance conducted by your affiant and other agents, along with other evidence and public records that I have reviewed, reveal that Kain also uses his residence, 16332 Horseshoe Drive, Northville, Michigan (SUBJECT PREMISES 2), as a place he conducts business and maintains business records. First, information received from the U.S. Postal Service shows that business mail addressed to Specialized Overseas Shipping is sent to SUBJECT PREMISES 2. Next, emails from Kain regarding SOS business obtained from a search warrant shows that Kain works from SUBJECT PREMISES 2 (his home) on occasion and has sent emails from his personal residence with attached business documents from SOS. Further, Kain sent an email in January of 2019 stating that he was working from home (SUBJECT PREMISES 2). Surveillance has also place KAIN at

SUBJECT PREMISES 2 during working hours over the last six months. Finally, Beydoun's occupation with SOS is listed as "secretary," and per surveillance, she has not worked at SOS's offices at all over the last six months; rather, surveillance indicates that she is at SUBJECT PREMISES 2 during business hours. Thus, there is probable cause that SOS business records are located at SUBJECT PREMISES 2. There is also probable cause that Kain and Beydoun's personal bank and tax information, subject to this warrant, will be located at SUBJECT PREMISES 2. First, information received from the U.S. Postal Service shows that personal financial mail for Kain and Beydoun is also sent to SUBJECT PREMISES 2, including mail from credit card companies, life insurance companies, and financial institutions. Second, SUBJECT PREMISES 2 is listed as the residence of record on Kain/Beydoun's personal tax filings. Based on my training and experience, people usually keep personal financial and tax information in their residence, here, SUBJECT PREMISES 2.

50. Thus, there is probable cause to believe that records and evidence further described in Attachment B will be located in SUBJECT PREMISES 2.

COMPUTERS, ELECTRONIC STORAGE, and FORENSIC ANALYSIS

51. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES in whatever form they are found. One form in which the records might be found is

data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

52. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, including financial information, vehicle sales records, and vehicle shipping records, I am aware that computer equipment was used to generate, store, and print documents used in the money laundering scheme. There is reason to believe that there is a computer system currently located on the SUBJECT PREMISES.

53. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may

indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

54. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the

computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

55. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or

otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

56. Specialized Overseas Shipping, SOS Transportation, and SOS Realty ("the Companies") are functioning companies that may conduct legitimate business. The seizure of the Companies' computers may limit the Companies' ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Companies' so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Companies' legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

CONCLUSION

36. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachments A-1 and A-2 and seize the items described in Attachment B.

37. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Jessica Knickerbocker

Jessica Knickerbocker, Special Agent
IRS – Criminal Investigations

Sword to before me and signed in my
presence and/or by reliable electronic means.

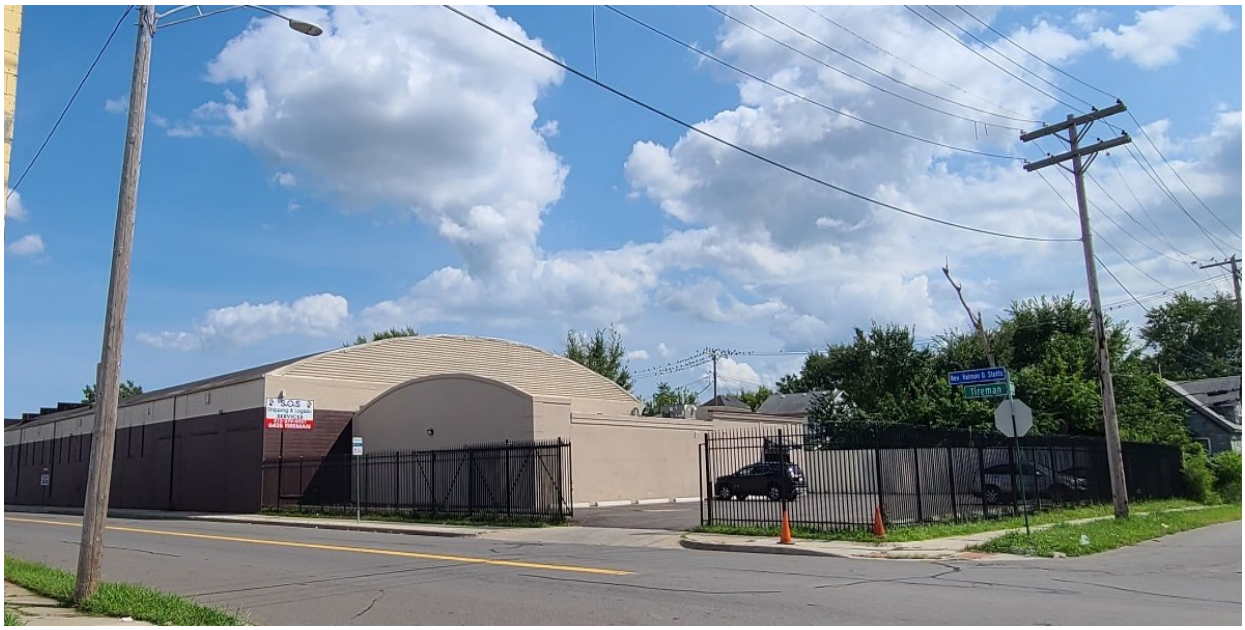
Anthony P. Patti
United States Magistrate Judge

Dated: October 12, 2021

ATTACHMENT A-1

DESCRIPTION OF THE PREMISES TO BE SEARCHED
SUBJECT PREMISES 1

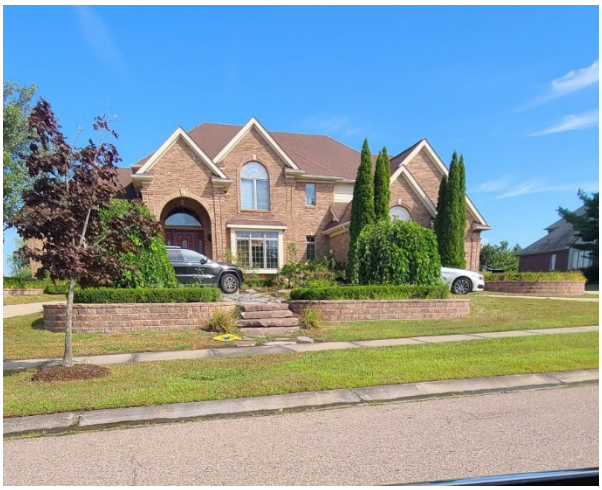
The property to be searched is a commercial business located at 6425 Tireman Street, Detroit, MI 48204. The commercial business is described as a brown and beige cinderblock warehouse. There are signs visible on the east and west side of the building that reads "S.O.S Shipping & Logistic SERVICES 313-279-0331 6425 TIREMAN." On the east side of the building are large garage doors for the loading/unloading of goods and/or vehicles. Also, on the east side of the building is a gated parking lot, that stores several vehicles. On the west side of the building is entry doors to the main office space along with a gated parking lot. There is an awning over the door that reads "OFFICE."

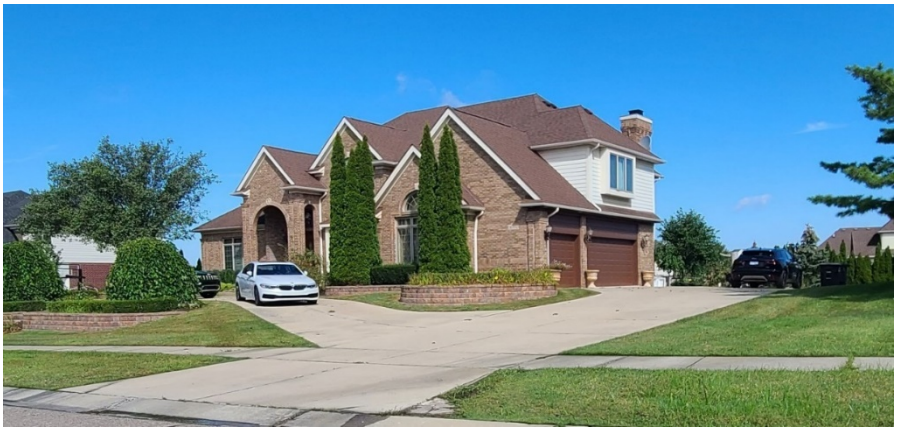


ATTACHMENT A-2

DESCRIPTION OF THE PREMISES TO BE SEARCHED
SUBJECT PREMISES 2

The property to be searched is residence located at 16332 Horseshoe Drive, Northville, MI 48168, belonging to Ali Kain and Mariam Beydoun. The residence has the numbers "16332" within on the brick located on the front of the home towards the east side of the residence by the garage. There is a three-car attached garage with side entrances on the east side of the home. The residence has a circle driveway.





ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. All items that constitute evidence, fruits, or instrumentalities of violations of 26 U.S.C. § 7206 (fraud and false statements) and 18 U.S.C. § 542 (entry of goods by means of false statements), from the period January 1, 2015, to the present, including but not limited to:

   a. Records and information related to the purchase and sale of vehicles including titles, bills of sale (RD-108), odometer statements, invoices, financing agreements, checks, money orders, wire transfers and sales tax records.

   b. Records and information relating to the shipment of vehicles including bills of lading, export declarations, customs forms, dock receipts, and shipping invoices.

   c. Records and information relating communication between or involving the persons named in this warrant including letters, phone messages, voice mail, e-mail, or other electronic communications.

   d. All financial documents, including:

      i. Any and all ledgers, journals, balance sheets, income statements, invoices, account books, records, billing statements, client/customer lists, calendars/digests, employee time records, payroll records, appointment books, vendor lists, checks, checkbooks, receipts, bills, phone recordings, contracts, leases, correspondence, cash register receipts, insurance summaries,

insurance records and other business/financial records of Ali Kain, Mariam Beydoun, Specialized Overseas Shipping (doing business as SOS), SOS Transportation, Inc., and SOS Realty, LLC.

ii. Any and all personal and business bank records including bank statements, cancelled checks, check registers, deposit tickets, debit and credit memos, checks deposited, withdrawal slips, and checks issued for withdrawals. All records and documents identifying the locations of safety deposit boxes including safety deposit keys, or other possible depositories for cash and other liquid assets which are identified in any way with Ali Kain, Mariam Beydoun, Specialized Overseas Shipping (doing business as SOS), SOS Transportation, Inc., and SOS Realty, LLC.

iii. Loan and/or mortgage records including applications; financial statements; loan agreements; loan contracts; checks issued for loans; repayment records including records revealing the date; amount, and method of repayment (cash or check); checks used to repay loans; promissory notes; amortization schedules; forbearance agreements; escrow agreements; correspondence between lending institutions and Ali Kain, Mariam Beydoun, Specialized Overseas Shipping (doing business as SOS), SOS Transportation, Inc., and SOS Realty, LLC.

iv. Personal and business credit card records, including: applications; monthly billing statements; individual charge invoices; repayment records disclosing the dates, amounts, and method of repayment (cash or check); and cancelled checks used to make repayments.

v. Any and all tax returns, tax information, tax schedules, copies of tax returns, and information returns of Ali Kain, Mariam Beydoun, Specialized Overseas Shipping (doing business as SOS), SOS Transportation, Inc., and SOS Realty, LLC. Also all retained copies of state and federal income or other tax returns, including Forms 1040, 1120, 1065, 1099, 940, 941, W-2, Schedules K-1 and supporting work papers, attachments, and summary sheets.

2. Electronically stored information: The above identified information and/or data may be stored in the form of magnetic or electronic coding on computer media, or on media capable of being read by a computer or with the aid of a computer related equipment. This media includes but is not limited to any magnetic or electronic storage device such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, electronic notebooks, cellular telephones/ Smartphones (Ali Kassem Kain's only). In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether or not these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

b. If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time and without jeopardizing the preservation of the data, then the computer personnel will determine whether it is practical to copy/image the data.

c. If the computer personnel determine it is not practical to perform an on-site searching, copying or imaging (due to time, technical or other considerations), then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) any data that falls within the list of items to be seized set forth within.

e. In searching the data, computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein.

f. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule

of Criminal Procedure 41(b), the government will return these items within a reasonable period of time.

g. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

- Any computer equipment and storage devices capable of being used to commit or store evidence of the offenses listed above;
- Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including but not limited to word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
- Any magnetic, electric or optical storage device capable of storing data such as floppy disks, hard disk tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, USB flash memory devices, personal digital assistants, mobile telephones or answering machines;
- Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices, or software;
- Any applications, utility programs, compliers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;
- Any physical keys, encryption devices and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

- Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices or data.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software (or the lack thereof) that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.

d. Evidence indicating the computer user's state of mind as it relates to the crime under investigation.

e. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence.

f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

g. Evidence of the times the COMPUTER was used.

h. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.

i. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER.

j. Records of or information about Internet Protocol addresses used by the COMPUTER.

k. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

l. Contextual information necessary to understand the evidence described in this attachment.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

USAO File Number: 2018R00729 AUSA: Hank Moon Telephone: (313) 226-9100

AO 93 (Rev. 11/13) Search and Seizure Warrant Special Agent: Jessica Knickerbocker Telephone: (313) 965-2323

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 6425 Tireman Street, Detroit, MI 48204, and 16332 Horseshoe Drive, Northville, MI 48168, more fully described in Attachments A-1 and A-2.	)	Case No. 19-mc-50186-5

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENTs A-1 and A-2.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B, violations of:

26 U.S.C. § 7206, fraud and false statements
18 U.S.C. § 542, entry of goods by means of false statements

YOU ARE COMMANDED to execute this warrant on or before October 26, 2021 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: October 12, 2021 5:20 pm

Judge's signature

City and state: Detroit, Michigan Anthony P. Patti U. S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 19-mc-50186-5	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title